

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claims 1, 3-14, 16, 18, 20-28, and 30-32 without prejudice or disclaimer in accordance with the following:

1. - 14. (CANCELLED)

15. (PREVIOUSLY PRESENTED) A data management system, comprising:
a storage medium for storing contents;
application executing means for activating an application so that the application accesses the contents stored in the storage medium and effects a processing on the contents;
access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application;

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application, and

wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other, and the access monitoring means monitors the status of access with the assistance of the management table, and

wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium, and

wherein

when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the inherent information for the contents, and

wherein

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents, with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names disagree with each other as the result of comparison, the access monitoring means changes a file name of the newly created file so that the newly created file is stored in the logical drive of the drive name registered in the management table and registers the changed file name in the management table.

16. (CANCELLED)

17. (PREVIOUSLY PRESENTED) A data management system, comprising:

a storage medium for storing contents;

application executing means for activating an application so that the application accesses the contents stored in the storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application;

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application, and

wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other, and the access monitoring means monitors the status of access with the assistance of the management table, and

wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium, and

wherein

when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the inherent information for the contents, and

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents, with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names are coincident with each other as the result of comparison, then the access monitoring means prohibits a file name of the newly created file from being registered in the management table.

18. (CANCELLED)

19. (PREVIOUSLY PRESENTED) A data management system, comprising:
a storage medium for storing contents;
application executing means for activating an application so that the application

accesses the contents stored in the storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application;

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application, and

wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other, and the access monitoring means monitors the status of access with the assistance of the management table, and

wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium, and

wherein

when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the inherent information for the contents, and

wherein

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on

the contents with a drive name of the logical drive registered in the management table, and
if it is determined that both of the drive names disagree with each other as the
result of comparison, then the operation of the filtering means is validated.

20. (CANCELLED)

21. (ORIGINAL) A data management system according to Claim 19, wherein
the storage medium comprises a primary storage means which erases data stored
therein upon power supply cut, and
the filtering means stores an enciphered version of the newly created file in the primary
storage means instead of the logical drive as the storage destination.

22. -32. (CANCELLED)